Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1.   (Currently Amended) A system that supports secure communication of data between an electronic device and a network, the system comprising:

an electronic device comprising:

a first component that manages information in the electronic device; and

a second component that provides access to proprietary information in the electronic device; and

at least one server that manages ~~the~~ information communicated to the electronic device via the network, a first portion of information and a second portion of information being used to securely communicate data to the electronic device, the first portion of information and the second portion of information being managed by the at least one server and the first component to provide secure communication between the electronic device and the network.

2.   (Original)   The system according to claim 1 wherein the first portion of information is a portion of information dynamically sent to the electronic device.

3.   (Original)   The system according to claim 2 wherein the first portion of information is communicated over a proprietary communication protocol.

4.   (Original)   The system according to claim 1 wherein the second portion of information is a portion of static information available to the electronic device.

5.   (Original)   The system according to claim 4 wherein the second portion of information is an electronic security number (ESN).

6.   (Original)   The system according to claim 4 wherein the second portion of information is provided by a subscriber identity module (SIM) card.

7.   (Original)   The system according to claim 1 wherein the first portion of information is combined with the second portion of information to generate encryption information.

8.   (Original)   The system according to claim 1 wherein the first portion of information comprises a first key and the second portion of information comprises a second key.

9.   (Original)   The system according to claim 8 wherein the first component retrieves the first key from the at least one server.

10.   (Original)   The system according to claim 8 wherein the at least one server sends the first key to the first component.

11.   (Original)   The system according to claim 8 wherein the at least one server generates the first key.

12.   (Original)   The system according to claim 8 wherein the first key is generated for the at least one server.

13.   (Original)   The system according to claim 8 wherein the first key and the second key are combined to provide a higher level of security in the system and the data communication between the electronic device and the network relative to using the first key and the second key separately.

14.   (Original)   The system according to claim 8 wherein the at least one server assembles a message that contains the first key and communicates the message to the electronic device.

15.   (Original)   The system according to claim 14 wherein the at least one server communicates with the electronic device via a proprietary communication protocol.

16.   (Original)   The system according to claim 14 wherein the electronic device processes the message to retrieve the first key.

17.   (Original)   The system according to claim 1 wherein the first component comprises:

>   a first agent that downloads data and information onto the electronic device;

>   a second agent that applies the downloaded data and information onto appropriate applications in the electronic device; and

>   a first manager that facilitates secure communications.

18.   (Original)   The system according to claim 17 wherein the electronic device further comprises a third component that facilitates downloads performed by the second agent of the first component of the electronic device.

19.   (Currently Amended) A   method   for   securely   communicating   data   and information between an electronic device and a network, the network comprising at least one server that manages communication via the network, the method comprising:

>   storing a first security key;

>   receiving a message containing a second security key;

>   processing the received message;

>   retrieving the second security key from the processed message; and

>   generating a third security key, wherein the electronic device combines the first security key and the second security key to generate the third security key.

20.   (Cancelled)

21.   (Original)   The method according to claim 19 wherein the method further comprises employing the third security key for communication with the at least one server.

22.   (Original)   The method according to claim 21 wherein the at least one server utilizes a copy of the third security key to decrypt information received from the electronic device.

23.   (Original)   The method according to claim 21 wherein the electronic device utilizes the third security key to decrypt data received from the at least one server.

24. (Original)   The method according to claim 21 wherein the method further comprises performing a security check to verify an access activity from the electronic device.

25. (Original)   The method according to claim 24 wherein the access activity from the electronic device comprises a request for information.

26. (Original)   The method according to claim 25 wherein the method further comprises processing the request of the electronic device.

27. (Previously Presented)   An electronic device comprising:

an integrated circuit card, wherein the electronic device performs secure firmware updates utilizing the integrated circuit card;

a first key, wherein the integrated circuit card provides the first key; and

wherein the electronic device employs the first key to authenticate information for updating firmware received from an external system.

28. (Previously Presented)   The electronic device according to claim 27, further comprising:

a manager that manages a life cycle of the first key; and

wherein the first manager is capable of being employed to at least one of: encrypt data sent to the external system and decrypt data received from the external system.

29. (Previously Presented)   The electronic device according to claim 28 wherein the external system comprises a management server.

30. (Previously Presented)   The electronic device according to claim 27 wherein the electronic device decrypts information for updating firmware based on at least a portion of the first key, and wherein the information for updating firmware is provided by the external system.

31. (Previously Presented)   The electronic device according to claim 27, wherein the electronic device decrypts information for updating firmware based on at least a

portion of the first key and at least a portion of a second key, and wherein the information for updating firmware is provided by the external system.

32.   (Previously Presented)   The electronic device according to claim 31, wherein the second key comprises a key that is one of: received by the electronic device and computed by the electronic device.

33.   (Currently Amended) The electronic device according to claim 27, wherein the integrated circuit card comprises one of: a SIM card and a ~~Smart~~ smart card.